NIST Crypto Standards: Are They For You?

Tim Polk

September 23, 2008

Overview

- NIST and cryptography
- NIST cryptographic publications
- Types of NIST crypto pubs
- When are NIST standards required?
- What if I use an alg that isn't NIST approved?

Cryptography is a Core Competency

- NIST published the Data Encryption Standard (DES) as FIPS in 1976.
- The Advanced Encryption Standard (AES) is published in 2001 as FIPS 197 after an international competition
- NIST is currently holding an international competition for an new secure hash algorithm

Types of NIST Cryptographic Publications

- FIPS publications that specify core cryptographic algorithms
  - block ciphers, secure hash algorithms, digital signature algorithms
- NIST Recommendations
  - Modes of operation, key derivation functions
- Validation related specifications
  - FIPS 140, Implementation Guidance
- Application specific guidance
  - SSL VPNs

Who Needs to Use NIST's Crypto Publications

- Federal agencies are required to use approved algorithms and validated modules
- External organizations are not required to use NIST pubs at all…
  - But lots of organizations choose to to rely on our standards voluntarily
- Why? Because the details *matter*

Security is Art *AND* Science

- Security is a mix of policy, procedures, and technology
- This makes it hard to quantify security
  - Separation of duties, physical security, and personnel security are important but its hard to put a number on them
- Cryptography promises quantifiable security
  - For example, “the Work factor of a brute force attack is 2^{80}”

Bad Cryptography Happens

- Sometimes it is a weak algorithm
  - History is littered with algorithms that turned out to be insecure
- Sometimes it is the protocol

We’re From the Government and We’re Here to Help!

- NIST’s cryptographic programs are designed to ensure that algorithms and products meet the government's requirements
- Are your cryptographic algorithms and products good enough to meet your requirements?

For more Information

- See
  - http://csrc.nist.gov/